Security assessment

Owner: Ho Yeung, Lee

Classification: Secret

FIPS-199 SC administrative information = {(confidentiality, HIGH), (integrity, LOW), (availability, LOW)}

Standard: NIST 800-115, NIST 800-53A, OWASP

Specifications are the documents associated with the system being audited. Speci- fications generally include policies, procedures, requirements, specifications, and designs.

Mechanisms are the controls used within an information system to meet the specifi- cations. Mechanisms may be based in hardware, software, or firmware.

Activities are the actions carried out by people within an information system. These may include performing backups, exporting log files, or reviewing account histories.

Individuals are the people who implement specifications, mechanisms, and activities.

Quantitative Risk Analysis

1. Inventory assets, and assign a value (asset value, or AV). (Asset value is detailed further in a later section of this chapter named “Asset Valuation.”)

2. Research each asset, and produce a list of all possible threats of each individual asset. For each listed threat, calculate the exposure factor (EF) and single loss expectancy (SLE).

SLE = asset value (AV) \* exposure factor (EF)

3. Perform a threat analysis to calculate the likelihood of each threat being realized within a single year—that is, the annualized rate of occurrence (ARO).

4. Derive the overall loss potential per threat by calculating the annualized loss expectancy (ALE).

ALE = single loss expectancy (SLE) \* annualized rate of occurrence (ARO)

5. Research countermeasures for each threat, and then calculate the changes to ARO and ALE based on an applied countermeasure.

6. Perform a cost/benefit analysis of each countermeasure for each threat for each asset. Select the most appropriate response to each threat.

Cost-benefit Analysis

* The pre-countermeasure ALE for an asset-and-threat pairing The post-countermeasure ALE for an asset-and-threat pairing The ACS (annual cost of the safeguard)
* With those elements, you can finally obtain a value for the cost/benefit formula for this specific safeguard against a specific risk against a specific asset:(pre-countermeasure ALE – post-countermeasure ALE) – ACS

Risk Responses

* Risk Mitigation
* Risk Assignment
* Risk Acceptance
* Deterrence
* Avoidance
* Reject or ignore

Countermeasure Selection and Implementation

Qualitative Risk Analysis

Log Reviews – NIST 800 - 115

* Authentication server or system logs may include successful and failed authentication attempts.
* System logs may include system and service startup and shutdown information, installation of unauthorized software, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and privilege use.
* Intrusion detection and prevention system logs may include malicious activity and inappropriate use.
* Firewall and router logs may include outbound connections that indicate compromised internal devices (e.g., rootkits, bots, Trojan horses, spyware).
* Firewall logs may include unauthorized connection attempts and inappropriate use.
* Application logs may include unauthorized connection attempts, account changes, use of privileges, and application or database usage information.
* Antivirus logs may include update failures and other indications of outdated signatures and software.
* Security logs, in particular patch management and some IDS and intrusion prevention system (IPS) products, may record information on known vulnerable services and applications.

Rule set review – NIST 800 - 115

For router access control lists

* Each rule is still required (for example, rules that were added for temporary purposes are removed as soon as they are no longer needed)
* Only traffic that is authorized per policy is permitted, and all other traffic is denied by default

For firewall rulesets

Each rule is still required

* Rules enforce least privilege access, such as specifying only required IP addresses and ports
* More specific rules are triggered before general rules
* There are no unnecessary open ports that could be closed to tighten the perimeter security
* The ruleset does not allow traffic to bypass other security defenses
* For host-based firewall rulesets, the rules do not indicate the presence of backdoors, spyware activity, or prohibited applications such as peer-to-peer file sharing programs

For IDS/IPS rule set

* Unnecessary signatures have been disabled or removed to eliminate false positives and improve performance
* Necessary signatures are enabled and have been fine-tuned and properly maintained.

System Configuration Review – NIST 800 - 115

File Integrity Checking – NIST 800 - 115

Account Management

1. Managers ask system administrators to provide a list of users with privileged access and the privileged access rights. They may monitor the administrator as they retrieve this list to avoid tampering.

2. Managers ask the privilege approval authority to provide a list of authorized users and the privileges they should be assigned.

3. The managers then compare the two lists to ensure that only authorized users retain access to the system and that the access of each user does not exceed their authorization.

Backup Verification

* reviewing logs,
* inspecting hash values,
* requesting an actual restore of a system or file.

Key Performance and Risk Indicators

* Number of open vulnerabilities
* Time to resolve vulnerabilities
* Vulnerability/defect recurrence
* Number of compromised accounts
* Number of software flaws detected in preproduction scanning
* Repeat audit findings
* User attempts to visit known malicious sites

Vulnerability assessment

Network Sniffing – NIST 800 - 115

Vulnerability Scan:

Technique:

1. TCP SYN Scanning Sends a single packet to each scanned port with the SYN flag set. This indicates a request to open a new connection. If the scanner receives a response that has the SYN and ACK flags set, this indicates that the system is moving to the second phase in the three-way TCP handshake and that the port is open. TCP SYN scanning is also known as “half-open” scanning.
2. TCP Connect Scanning Opens a full connection to the remote system on the specified port. This scan type is used when the user running the scan does not have the necessary permissions to run a half-open scan. Most other scan types require the ability to send raw packets, and a user may be restricted by the operating system from sending handcrafted packets.
3. TCP ACK Scanning Sends a packet with the ACK flag set, indicating that it is part of an open connection. This type of scan may be done in an attempt to determine the rules enforced by a firewall and the firewall methodology.
4. Xmas Scanning Sends a packet with the FIN, PSH, and URG flags set. A packet with so many flags set is said to be “lit up like a Christmas tree,” leading to the scan’s name.

network discovery scans

* Open The port is open on the remote system and there is an application that is actively accepting connections on that port.
* Closed The port is accessible on the remote system, meaning that the firewall is allowing access, but there is no application accepting connections on that port.
* Filtered Nmap is unable to determine whether a port is open or closed because a firewall is interfering with the connection attempt.

Best is FILTERED

network vulnerability scans

web application vulnerability scans

database vulnerability scans